This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1-20 (Cancelled)

21(New). A method for safely authenticating a user on line by a specific server through a terminal selected from a mobile phone, a PC and a bank cash dispenser, the method comprising the steps of:
(a) generating at the server an image table in which two or more key images and other images that are previously designated on a user basis are randomly mixed and transmitting the image table to a screen of the user's terminal; and
(b) if the key images are validly selected and inputted from the terminal, approving authentication of the user at the server,
wherein the procedure of selecting the key images is not displayed on the image table in the screen of the terminal.

22(New). A method for safely authenticating a user by a lock device selected from a door lock and a safe, the method comprising the steps of:
(a) generating and outputting at the lock device an image table in which two or more key images and other images that are previously designated are randomly mixed; and
(b) if the key images are validly selected and inputted from an input unit, approving authentication of the user and releasing the locking state at the lock device, wherein the procedure of selecting the key images is not displayed on the image table in the screen of the lock device.

23(New). The method as recited in claim 21, further comprising, before said step (a), an access location tracking step (c) in which a program that performs a function of

tracking an access location of the terminal on-line is automatically installed and executed in the terminal from the server connected to the terminal, and access location information of the terminal is sent and stored in the server.

24(New). The method as recited in claim 23, further comprising the step (d) of reporting access location information on online of another person acquired through the step (c) to the user when another person proceeds with the step (b) by using the authentication information of the user in a state that the authentication of the user is approved at the server and being connected.

25(New). The method as recited in claim 23, further comprising, after the step (b), the step (e) of reporting the latest access location information to the user's terminal.

26(New). The method as recited in claim 21, wherein the image table provided by the attempt of authentication of the user is different from an image table provided by the previous attempt of authentication.

27(New). The method as recited in claim 22, wherein the image table provided by the attempt of authentication of the user is different from an image table provided by the previous attempt of authentication.

28(New). The method as recited in claim 21, wherein start coordinates (initially inputted key image coordinates) at said step (b) are previously designated as one of the key images.

29(New). The method as recited in claim 22, wherein start coordinates (initially inputted key image coordinates) at said step (b) are previously designated as one of the key images.

30(New). The method as recited in claim 21, wherein the authentication approval at said step (b) is made in such a way that the corresponding key images are sequentially inputted by movement of coordinates in the image table based on a predetermined input sequence of the key images.

31(New). The method as recited in claim 22, wherein the authentication approval at said step (b) is made in such a way that the corresponding key images are sequentially inputted by movement of coordinates in the image table based on a predetermined input sequence of the key images.

32(New). The method as recited in claim 30, wherein start coordinates (initially inputted key image coordinates) at said step (b) are designated as coordinates of a first key image of the key images.

33(New). The method as recited in claim 31, wherein start coordinates (initially inputted key image coordinates) at said step (b) are designated as coordinates of a first key image of the key images.

34(New). The method as recited in claim 21, wherein, before said step (a), the server constructs and registers a personalization image table which is formed by selecting the key image and other images constituting the image table individually on a user basis.

35(New). The method as recited in claim 22, wherein, before said step (a), the lock device constructs and registers a personalization image table which is formed by selecting the key image and other images constituting the image table individually on a user basis.

36(New). The method as recited in claim 34, wherein, when the user selects the key images, and a passage coordinate image or a terminal coordinate image,

the server constructs the personalization image table by randomly extracting from remaining images excepting the selected images.

37(New). The method as recited in claim 35, wherein, when the user selects the key images, and a passage coordinate image or a terminal coordinate image,
the lock device constructs the personalization image table by randomly extracting from remaining images excepting the selected images.

38(New). The method as recited in any one of claims 21, wherein the server acquires IP information of a terminal accessed prior to said step (b), and notifies, if the key images of the user are not validly inputted from said step (b), an alarm message including the IP information to the user.

39(New). A method for safely authenticating a user on line by a specific server through a terminal selected from a mobile phone, a PC and a bank cash dispenser, the method comprising a login step of inputting an ID and a password of the user by the input of text through the terminal, and the method comprising the steps of:
(a) generating at the server an image table in which two or more key images and other images that are previously designated on a user basis are randomly mixed and transmitting the image table to a screen of the user's terminal; and
(b) if the key images are validly selected and inputted from the terminal, approving authentication of the user at the server,
wherein the procedure of selecting the key images is not displayed on the image table in the screen of the terminal.

40(New). A method for safely authenticating a user by a lock device selected from a door lock and a safe, the method comprising a login step of inputting an ID and a password of the user by the input of text through the lock device, and the method comprising the steps of:

(a) generating and outputting at the lock device an image table in which two or more key images and other images that are previously designated are randomly mixed; and

(b) if the key images are validly selected and inputted from an input unit, approving authentication of the user and releasing the locking state at the lock device, wherein the procedure of selecting the key images is not displayed on the image table in the screen of the lock device.

41(New). The method as recited in claim 39, further comprising, before said step (a), an access location tracking step (c) in which a program that performs a function of tracking an access location of the terminal on-line is automatically installed and executed in the terminal from the server connected to the terminal, and access location information of the terminal is sent and stored in the server.

42(New). The method as recited in claim 41, further comprising the step (d) of reporting access location information on online of another person acquired through the step (c) to the user when another person proceeds with the step (b) by using the authentication information of the user in a state that the authentication of the user is approved at the server and being connected.

43(New). The method as recited in claim 41, wherein the image table provided by the attempt of authentication of the user is different from an image table provided by the previous attempt of authentication.

44(New). The method as recited in claim 39, wherein start coordinates (initially inputted key image coordinates) at said step (b) are previously designated as one of the key images.

45(New). The method as recited in claim 40, wherein start coordinates (initially inputted key image coordinates) at said step (b) are previously designated as one of the key images.

46(New). The method as recited in claim 39, wherein the authentication approval at said step (b) is made in such a way that the corresponding key images are sequentially inputted by movement of coordinates in the image table based on a predetermined input sequence of the key images.

47(New). The method as recited in claim 40, wherein the authentication approval at said step (b) is made in such a way that the corresponding key images are sequentially inputted by movement of coordinates in the image table based on a predetermined input sequence of the key images.

48(New). The method as recited in claim 47, wherein start coordinates (initially inputted key image coordinates) at said step (b) are designated as coordinates of a first key image of the key images.

49(New). The method as recited in claim 39, wherein, before said step (a), the server constructs and registers a personalization image table which is formed by selecting the key image and other images constituting the image table individually on a user basis.

50(New). The method as recited in claim 40, wherein, before said step (a), the lock device constructs and registers a personalization image table which is formed by selecting the key image and other images constituting the image table individually on a user basis.